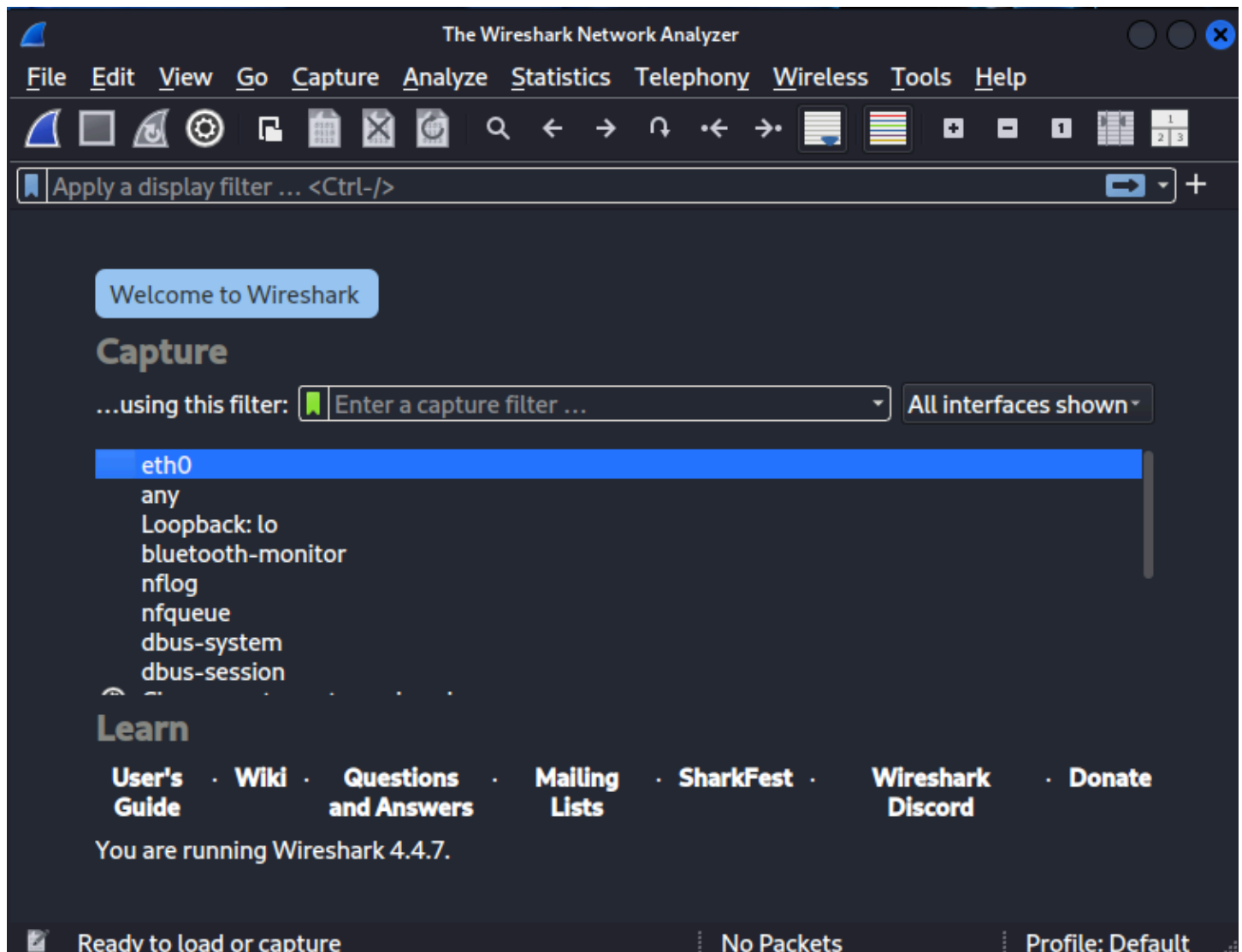


ELEVATE LABS CYBER SECURITY INTERNSHIP

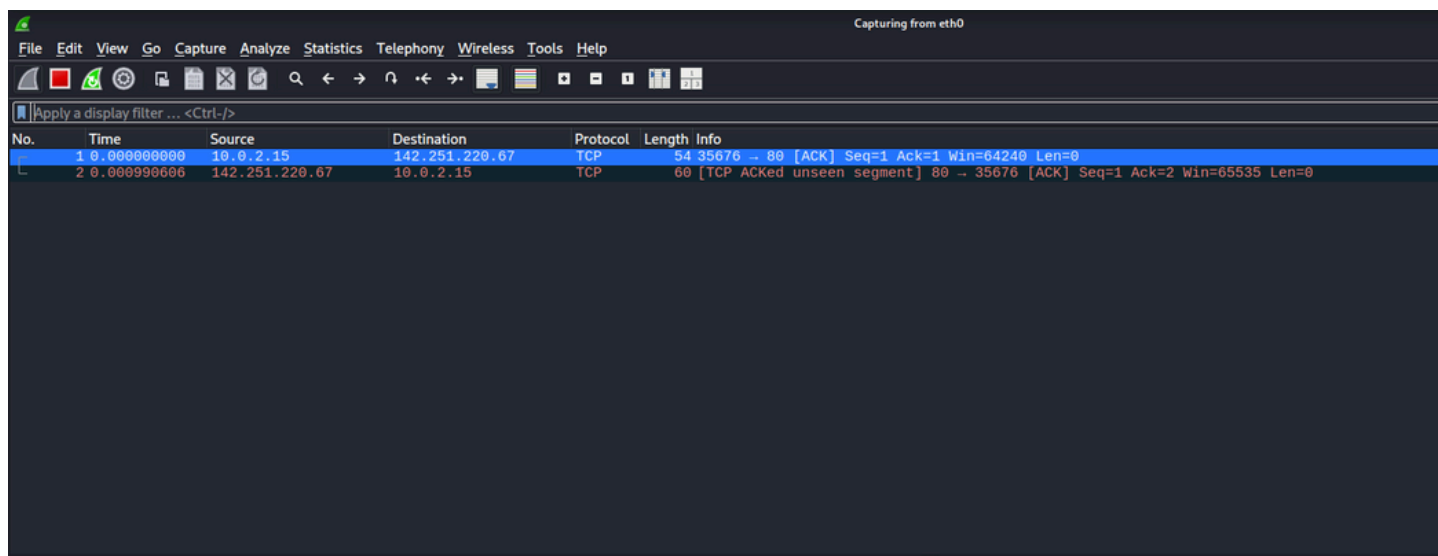
Task-5:

1.Install Wireshark.

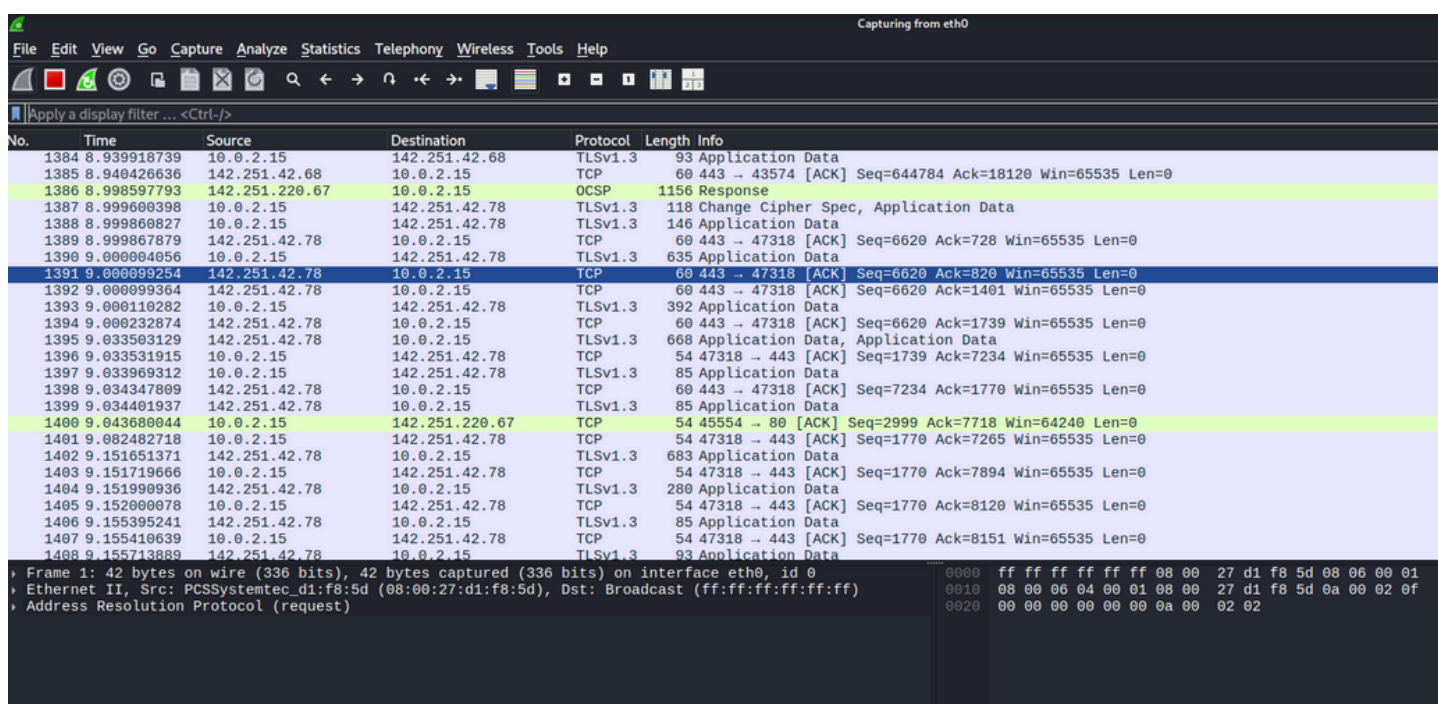
It is an inbuilt tool in the kali linux.



2.Start capturing on your active network interface.



3. Browse a website or ping a server to generate traffic.



4. Stop capture after a minute.

5. Filter captured packets by protocol.

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	142.251.220.67	TCP	54	35676 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2	0.000990606	142.251.220.67	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 35676 [ACK] Seq=1 Ack=2 Win=65535 Len=0
3	1.537793566	10.0.2.15	34.107.221.82	TCP	54	38390 → 80 [ACK] Seq=1 Ack=1 Win=64024 Len=0
4	1.538086683	34.107.221.82	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 38390 [ACK] Seq=1 Ack=2 Win=65535 Len=0
5	2.814383396	10.0.2.15	142.250.192.81	TLSv1.2	93	Application Data
6	2.814586285	10.0.2.15	142.250.192.131	TLSv1.2	93	Application Data
7	2.814864337	142.250.192.81	10.0.2.15	TCP	60	443 → 60794 [ACK] Seq=1 Ack=40 Win=65535 Len=0
8	2.814864581	142.250.192.131	10.0.2.15	TCP	60	443 → 58764 [ACK] Seq=1 Ack=40 Win=65535 Len=0
9	2.843990891	142.250.192.131	10.0.2.15	TLSv1.2	93	Application Data
10	2.843991212	142.250.192.81	10.0.2.15	TLSv1.2	93	Application Data
11	2.844027241	10.0.2.15	142.250.192.131	TCP	54	58764 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
12	2.894108445	10.0.2.15	142.250.192.81	TCP	54	60794 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
13	3.070857526	10.0.2.15	23.48.226.17	TCP	54	34236 → 80 [ACK] Seq=1 Ack=1 Win=63351 Len=0
14	3.071147466	23.48.226.17	10.0.2.15	TCP	60	[TCP ACKed unseen segment] 80 → 34236 [ACK] Seq=1 Ack=2 Win=65535 Len=0
15	3.821425877	10.0.2.15	142.251.42.234	TLSv1.2	93	Application Data
16	3.821544752	10.0.2.15	142.251.42.234	TLSv1.2	93	Application Data
17	3.822298877	142.251.42.234	10.0.2.15	TCP	60	443 → 40366 [ACK] Seq=1 Ack=40 Win=65535 Len=0
18	3.822299392	142.251.42.234	10.0.2.15	TCP	60	443 → 40362 [ACK] Seq=1 Ack=40 Win=65535 Len=0
19	3.858732417	142.251.42.234	10.0.2.15	TLSv1.2	93	Application Data
20	3.863214318	142.251.42.234	10.0.2.15	TLSv1.2	93	Application Data
21	3.904721863	10.0.2.15	142.251.42.234	TCP	54	40362 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
22	3.904753764	10.0.2.15	142.251.42.234	TCP	54	40366 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
23	4.825915226	10.0.2.15	142.251.42.78	TLSv1.2	93	Application Data
24	4.825980559	10.0.2.15	142.251.42.78	TLSv1.2	93	Application Data
25	4.826002154	10.0.2.15	142.251.42.68	TLSv1.2	93	Application Data

▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.251.220.67
 ▶ Transmission Control Protocol, Src Port: 35676, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

```

0000  52 54 00 12 35 02 08 00  27 d1 f8 5d 08 00 45 00  RT=5...[...]-E-
0010  00 3f eb 28 40 00 40 11  85 63 0a 00 02 0f ac 11  ?(00...c.....
0020  12 02 ec a0 00 35 00 2b  ca 5e a5 dc 01 00 00 01  .....5+...A.....
0030  00 00 00 00 00 00 05 66  6f 6e 74 73 07 67 73 74  .....f onts gst
0040  61 74 69 63 03 63 6f 6d  00 00 01 00 01          atic com .....
  
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
109	34.530752736	10.0.2.15	172.17.18.2	DNS	77	Standard query 0xa5dc A fonts.gstatic.com
110	34.530822345	10.0.2.15	172.17.18.2	DNS	77	Standard query 0x8edf AAAA fonts.gstatic.com
111	34.533720829	172.17.18.2	10.0.2.15	DNS	93	Standard query response 0xa5dc A fonts.gstatic.com A 142.251.221.227
112	34.534108843	172.17.18.2	10.0.2.15	DNS	105	Standard query response 0x8edf AAAA fonts.gstatic.com AAAA 2404:6800:4009:80d::2903

▶ Frame 109: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.17.18.2
 ▶ User Datagram Protocol, Src Port: 60576, Dst Port: 53
 ▶ Domain Name System (query)

```

0000  52 54 00 12 35 02 08 00  27 d1 f8 5d 08 00 45 00  RT=5...[...]-E-
0010  00 3f eb 28 40 00 40 11  85 63 0a 00 02 0f ac 11  ?(00...c.....
0020  12 02 ec a0 00 35 00 2b  ca 5e a5 dc 01 00 00 01  .....5+...A.....
0030  00 00 00 00 00 00 05 66  6f 6e 74 73 07 67 73 74  .....f onts gst
0040  61 74 69 63 03 63 6f 6d  00 00 01 00 01          atic com .....
  
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
tls							
No.	Time	Source	Destination	Protocol	Length	Info	
5	2.814383396	10.0.2.15	142.250.192.81	TLSv1.2	93	Application	Data
6	2.814586285	10.0.2.15	142.250.192.131	TLSv1.2	93	Application	Data
9	2.843990891	142.250.192.131	10.0.2.15	TLSv1.2	93	Application	Data
10	2.843991212	142.250.192.81	10.0.2.15	TLSv1.2	93	Application	Data
15	3.821425877	10.0.2.15	142.251.42.234	TLSv1.2	93	Application	Data
16	3.821544752	10.0.2.15	142.251.42.234	TLSv1.2	93	Application	Data
19	3.858732417	142.251.42.234	10.0.2.15	TLSv1.2	93	Application	Data
20	3.863214318	142.251.42.234	10.0.2.15	TLSv1.2	93	Application	Data
23	4.825915226	10.0.2.15	142.251.42.78	TLSv1.2	93	Application	Data
24	4.825980559	10.0.2.15	142.251.42.78	TLSv1.2	93	Application	Data
25	4.826002154	10.0.2.15	142.251.42.68	TLSv1.2	93	Application	Data
29	4.847120846	142.251.42.78	10.0.2.15	TLSv1.2	93	Application	Data
30	4.860044111	142.251.42.78	10.0.2.15	TLSv1.2	93	Application	Data
31	4.869139626	142.251.42.68	10.0.2.15	TLSv1.2	93	Application	Data
59	24.946457694	10.0.2.15	34.49.51.44	TLSv1.2	93	Application	Data
60	24.946721116	10.0.2.15	151.101.129.91	TLSv1.2	100	Application	Data
61	24.946777490	10.0.2.15	34.160.144.191	TLSv1.2	100	Application	Data
62	24.946825427	10.0.2.15	34.149.100.209	TLSv1.2	93	Application	Data
63	24.946877619	10.0.2.15	35.190.72.216	TLSv1.2	93	Application	Data
69	24.962765186	35.190.72.216	10.0.2.15	TLSv1.2	93	Application	Data
70	24.968974784	34.49.51.44	10.0.2.15	TLSv1.2	93	Application	Data
71	24.969672710	34.160.144.191	10.0.2.15	TLSv1.2	100	Application	Data
72	24.969672938	34.149.100.209	10.0.2.15	TLSv1.2	93	Application	Data
73	24.975187086	151.101.129.91	10.0.2.15	TLSv1.2	100	Application	Data

6. Identify at least 3 different protocols in the capture.

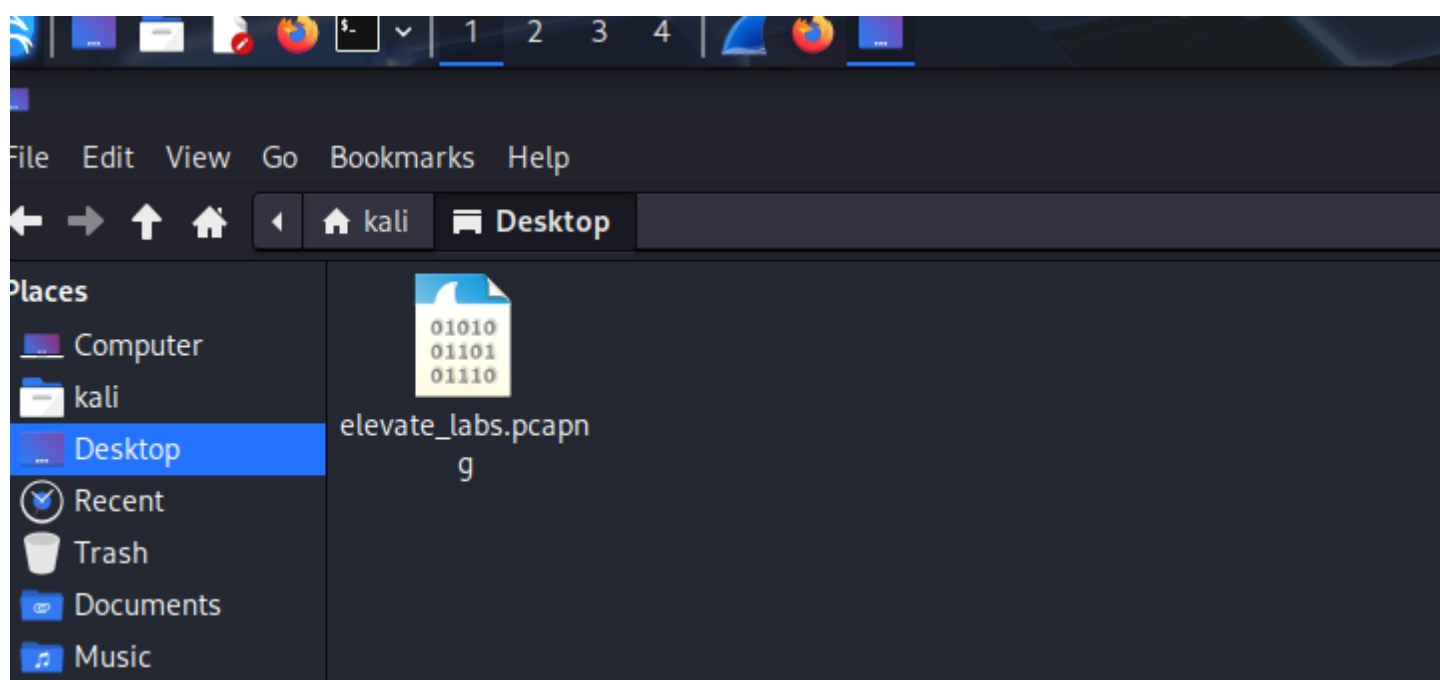
→ TCP

→ UDP

→ TLS

7. Export the capture as a .pcap file.

saved the file as elevate_labs.pcap



8. Summarize your findings and packet details.

The Wireshark packet capture shows a network session that includes TCP, TLSv1.2, and application data packets. The data is exchanged between a local IP address and an external IP, which means a secure connection is happening — likely for a website or app. The packet sizes range from small to medium, and many of them have sequence and acknowledgment numbers. Some packets are control messages that don't carry data. One highlighted packet shows a TCP segment with specific source and destination ports, sequence and acknowledgment numbers, and a small amount of data. Since it uses TLSv1.2 encryption, it's clear that this is a secure communication session, involving both data transfer and control messages.